Aerohive HiveManager NG Configuration Guide

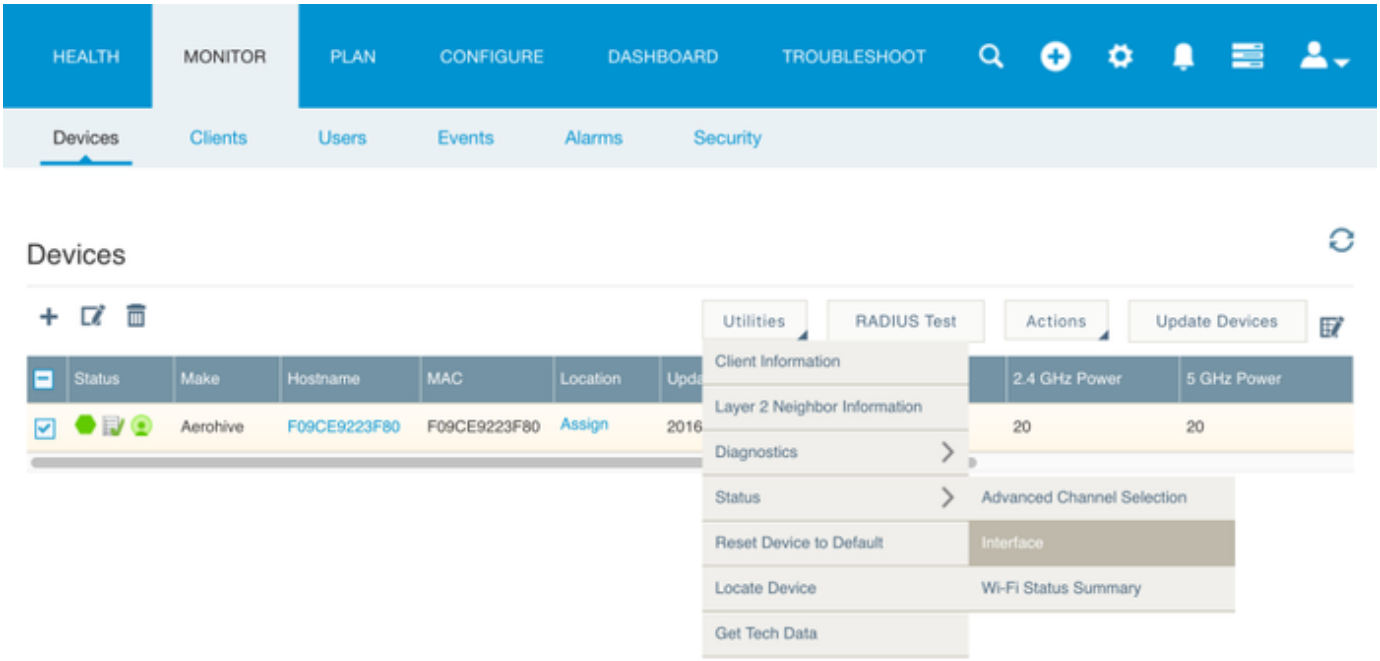
Creating Router for Business

Due to limitations, when connecting to the Zenreach portal, Aerohive devices report MAC address of the WIFI interface associated with the SSID that the user is connected for identification, instead of the WAN MAC address. Therefore for accuracy a new router must be created for each WIFI interface that hosts an SSID. Follow the steps listed below to obtain the list of WIFI MAC addresses.

Obtaining WIFI MAC addresses

Under the **`MONITOR`** tab, highlight the device and select **`Utilities`** - **`Status`** - **`Interface`**. You will then be presented with a popup window listing all the available interfaces on the device and their respective MAC addresses. Record the MAC addresses of the **`Mgt0/Eth0`** interface, as well as interfaces associated with the guest WiFi SSID. In this example below it would be the MAC addresses for **`Mgt0/Eth0`**, **`Wifi0.1`** and **`Wifi1.1`**.

Copy all relevant MAC addresses found on this page and email it to your Zenreach Account Manager. Please also email a screenshot of the interface to your Account Manager for our records. Without completion of this step, guests will receive a "404" or "Not Found" error on the captive portal.



Interface-F09CE9223F80
Interface Name
All
State=Operational state; Chan=Channel;
Radio=Radio profile; U=up; D=down;
Name MAC addr Mode State Chan(Width) VLAN Radio Hive SSID
Mgt0 f09c:e922:3f80 - U - 1 - Hive-Pr... -
Eth0 f09c:e922:3f80 backhaul U - 1 - Hive-Pr... -
Wifi0 f09c:e922:3f90 access U 7(20MHz) - radio_n... - -
Wifi0.1 f09c:e922:3f94 access U 7(20MHz) - radio_n... Hive-Pr... Aerohiv...
Wifi1 f09c:e922:3fa4 access U 40(20MHz) - radio_n... - -
Wifi1.1 f09c:e922:3fa8 access U 40(20MHz) - radio_n... Hive-Pr... Aerohiv...

[Send this screenshot of your interface to your Zenreach Account Manager]

Configuration

Create Captive Web Portal profile

- Under the **`CONFIGURE`** tab, go to **`Common Objects`** sub-tab. From the left hand side menu **`AUTHENTICATION`** - **`Captive Web Portals`** - **`Add a new captive web portal`**.

  For the 'mac' parameter, use any of the MAC addresses obtained from the above step.

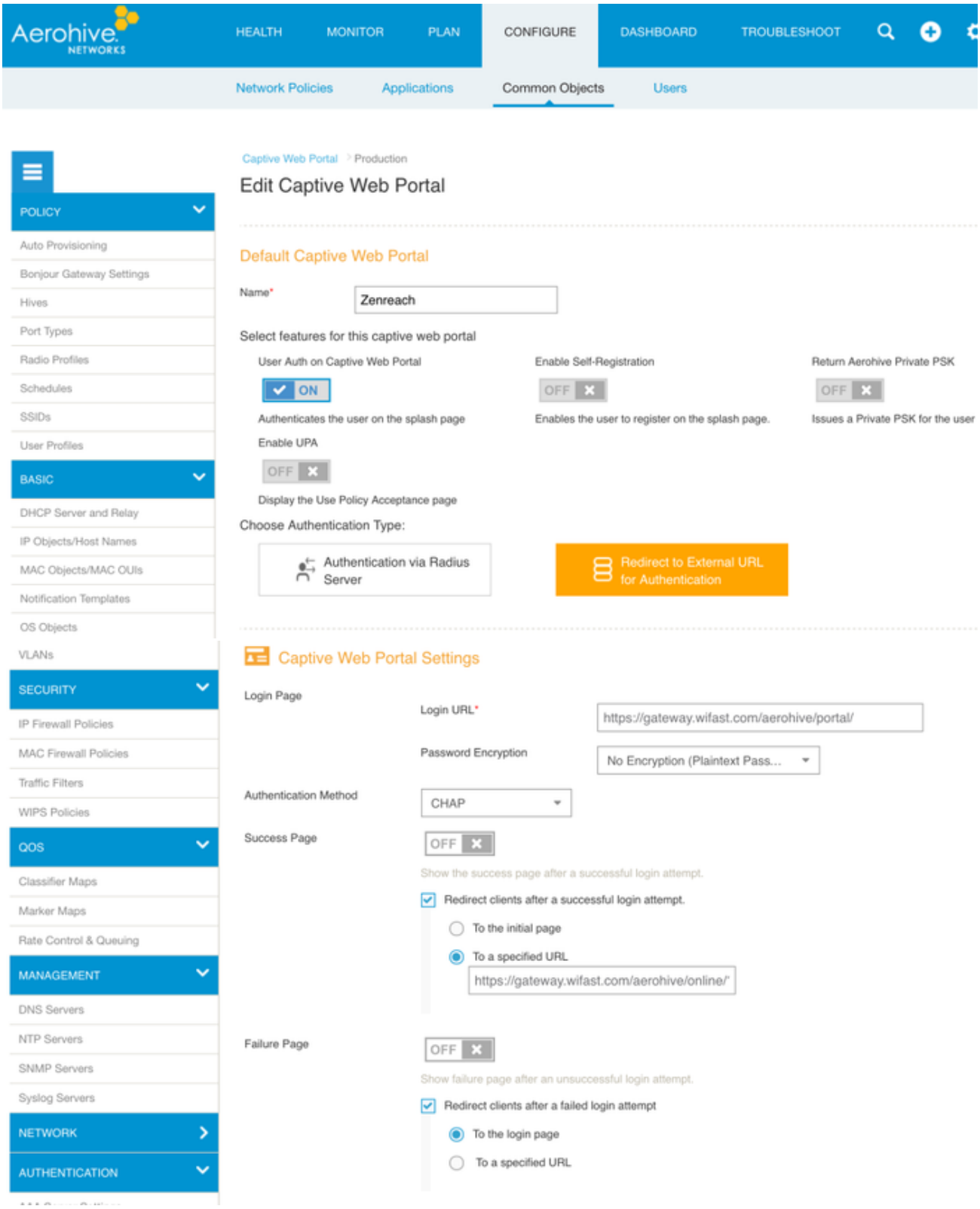
  [Note. The 'mac' parameter for the success redirect URL is to be able to the business information. If this is not specified then business related information will not be populated on the online page. This means that it is not necessary to create one captive portal for each AP and any AP WIFI MAC for a particular business that was previously registered with Zenreach can be used.]

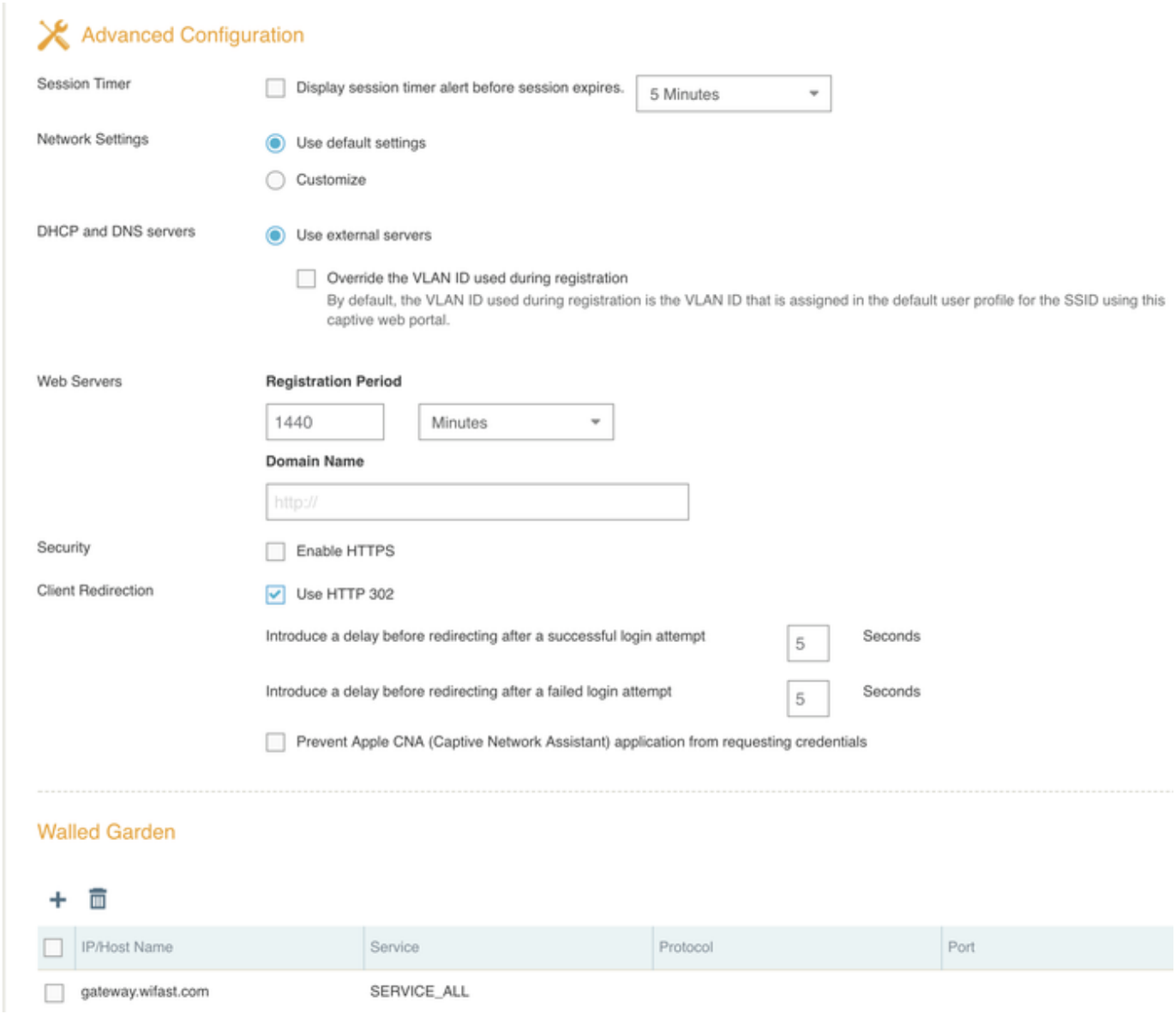
  Name: Zenreach
  User Auth on Captive Web Portal: [ON]
  Choose Authentication Type: [Redirect to External URL for Authentication]

  Captive Web Portal Settings
  Login Page
  Login URL: https://gateway.wifast.com/aerohive/portal/
  Authentication Method: CHAP
  Success Page: [OFF]
  Redirect clients after a successful login attempt: <checked>
  To a specified URL: https://gateway.wifast.com/aerohive/online/?mac=<insert any AP WIFI MAC here>
  Failure Page: [OFF]
  Redirect clients after a failed login attempt: <checked>
  To the login page: <selected>

  Advanced Configuration
  Web Servers
  Registration Period: 1440 Minutes
  Client Redirection: [Use HTTP 302]

  Walled Garden
  Add:
  IP Object/Host Name: gateway.wifast.com
  Service: All


Aerohive NETWORKS
HEALTH
MONITOR
PLAN
CONFIGURE
DASHBOARD
TROUBLESHOOT
Network Policies
Applications
Common Objects
Users
POLICY
Auto Provisioning
Bonjour Gateway Settings
Hives
Port Types
Radio Profiles
Schedules
SSIDs
User Profiles
BASIC
DHCP Server and Relay
IP Objects/Host Names
MAC Objects/MAC OUIs
Notification Templates
OS Objects
VLANs
SECURITY
IP Firewall Policies
MAC Firewall Policies
Traffic Filters
WIPS Policies
QOS
Classifier Maps
Marker Maps
Rate Control & Queuing
MANAGEMENT
DNS Servers
NTP Servers
SNMP Servers
Syslog Servers
NETWORK
AUTHENTICATION
Captive Web Portal > Production
Edit Captive Web Portal
Default Captive Web Portal
Name*
Zenreach
Select features for this captive web portal
User Auth on Captive Web Portal
ON
Authenticates the user on the splash page
Enable Self-Registration
OFF
Enables the user to register on the splash page.
Return Aerohive Private PSK
OFF
Issues a Private PSK for the user
Enable UPA
OFF
Display the Use Policy Acceptance page
Choose Authentication Type:
Authentication via Radius Server
Redirect to External URL for Authentication
Captive Web Portal Settings
Login Page
Login URL*
https://gateway.wifast.com/aerohive/portal/
Password Encryption
No Encryption (Plaintext Pass...
Authentication Method
CHAP
Success Page
OFF
Show the success page after a successful login attempt.
Redirect clients after a successful login attempt.
To the initial page
To a specified URL
https://gateway.wifast.com/aerohive/online/*
Failure Page
OFF
Show failure page after an unsuccessful login attempt.
Redirect clients after a failed login attempt
To the login page
To a specified URL



Create RADIUS Servers

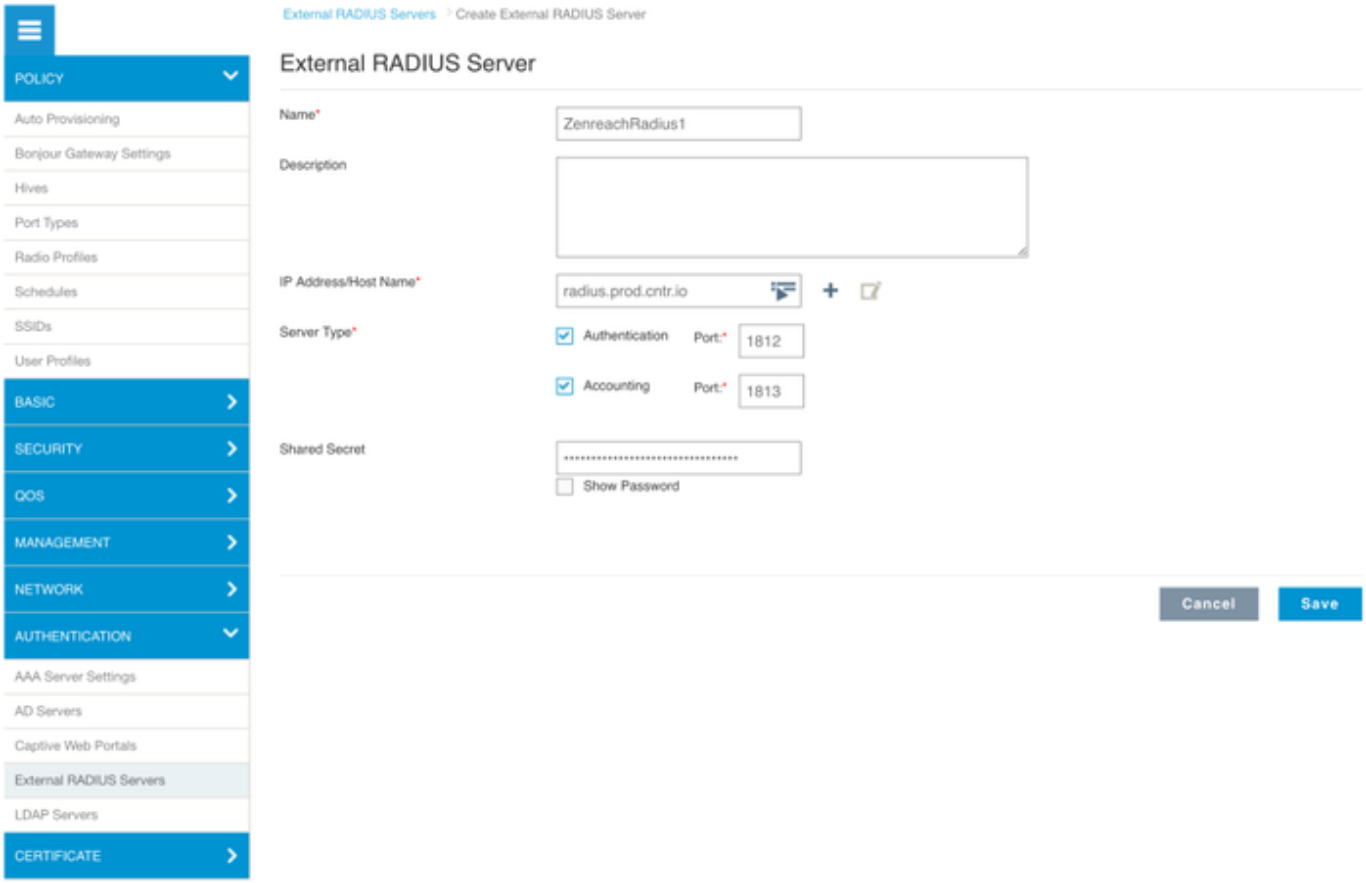
- Also under **`CONFIGURE`** - **`Common Objects`** - **`AUTHENTICATION`**, select **`External RADIUS Servers`** and add the following entries:

  Name: ZenreachRadius1
  IP Address/Host Name: radius.prod.cntr.io
  Server Type
  Authentication: <checked>
  Port: 1812
  Accounting: <checked>
  Port: 1813
  Shared Secret: 8fc40973252c42e196489d4a16849ff8

  Name: ZenreachRadius2
  IP Address/Host Name: 54.69.8.147
  Server Type
  Authentication: <checked>
  Port: 1812
  Accounting: <checked>
  Port: 1813
  Shared Secret: 8fc40973252c42e196489d4a16849ff8

  Name: ZenreachRadius3
  IP Address/Host Name: 54.68.29.80

Server Type
Authentication: <checked>
Port: 1812
Accounting: <checked>
Port: 1813
Shared Secret: 8fc40973252c42e196489d4a16849ff8

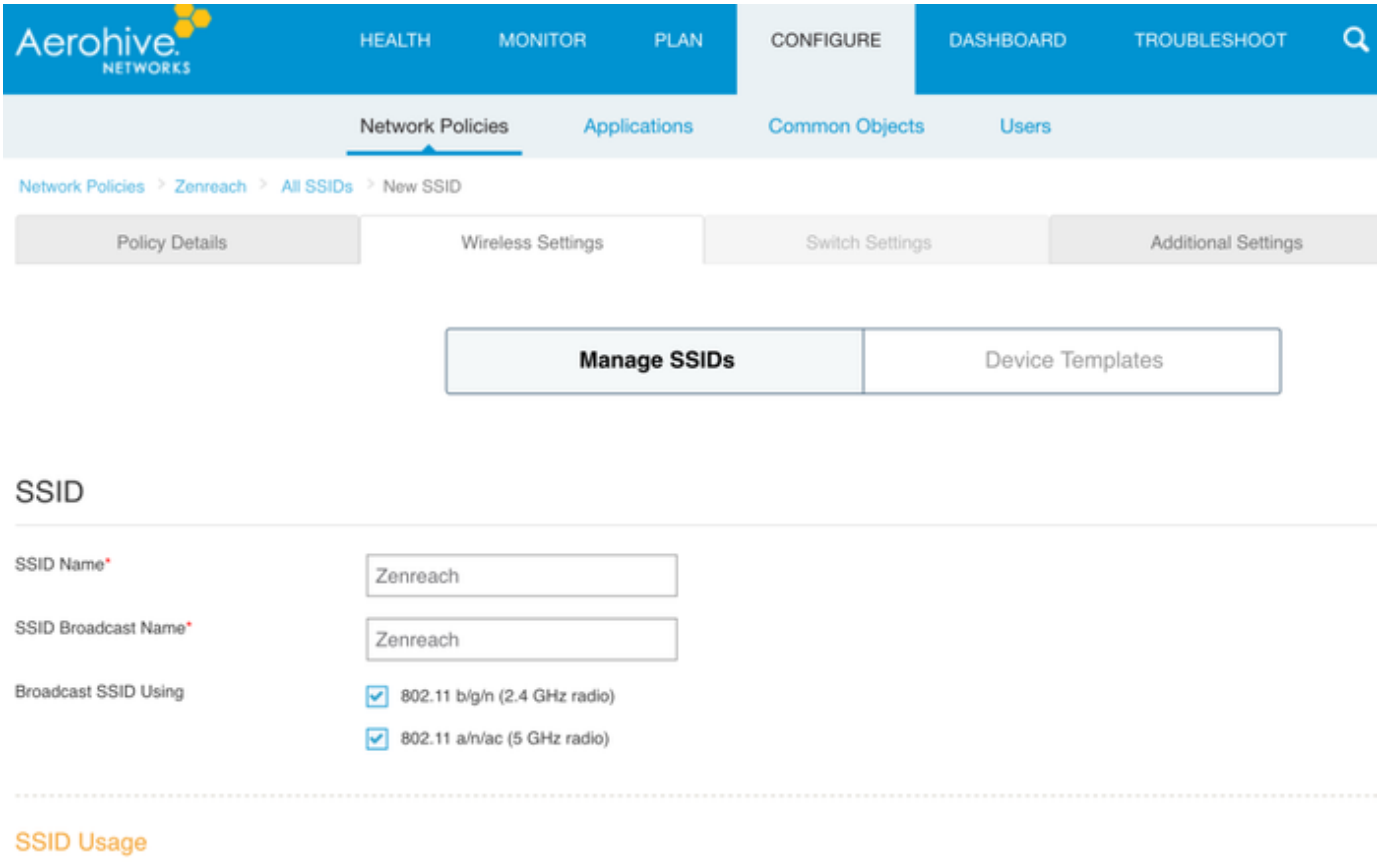


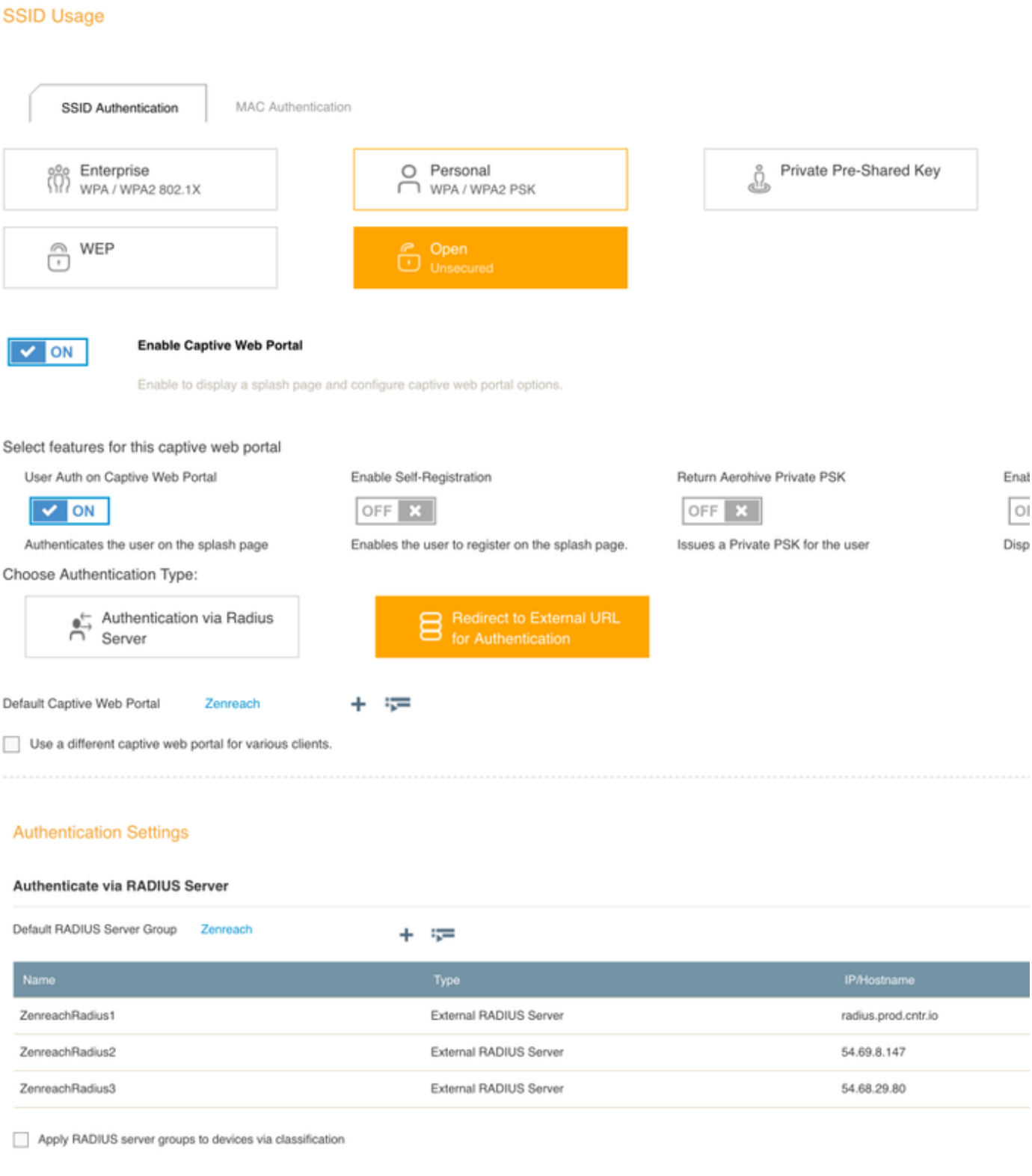
Configure Network Policy

- Under the **`CONFIGURE`** tab, **`Network Policies`** sub-tab, select the Network Policy you wish to have Zenreach hotspot support enabled.
    1. Policy Details
        a. What type of policy are you creating: [Wireless]
    2. Wireless Settings - Select (or create) an SSID for Zenreach hotspot support and check "Enable Captive Web Portal". Below
        a. **SSID Name**: Zenreach
        SSID Broadcast Name: Zenreach
        Broadcast SSID Using: 802.11 b/g/n (2.4 GHz radio), 802.11 a/n/ac (5 GHz radio)
        SSID Authentication: [Open]
        Enable Captive Web Portal: [ON]
        Select features for this captive web portal:
        User Auth on Captive Web Portal: [ON]
        Choose Authentication Type: [Redirect to External URL for Authentication]
        Default Captive Web Portal: [Zenreach]

        Authentication Settings
        Authenticate via RADIUS Server
        Default RADIUS Server Group: Add a new RADIUS
        Server Group
        Name: Zenreach

        Server List: Select [ZenreachRadius1], [ZenreachRadius2], [ZenreachRadius3]


Aerohive NETWORKS
HEALTH
MONITOR
PLAN
CONFIGURE
DASHBOARD
TROUBLESHOOT
Network Policies
Applications
Common Objects
Users
Network Policies > Zenreach > All SSIDs > New SSID
Policy Details
Wireless Settings
Switch Settings
Additional Settings
Manage SSIDs
Device Templates
SSID
SSID Name*
Zenreach
SSID Broadcast Name*
Zenreach
Broadcast SSID Using
802.11 b/g/n (2.4 GHz radio)
802.11 a/n/ac (5 GHz radio)
SSID Usage



- Under the **`Optional Settings`** category, click the **`Customize`** button for **`Optional Settings`**.
- Set **`Inactive client ageout`** to **`30`** minutes.

- Deploy Policy to device.

Walled Garden for Social Login

A walled garden is a list of websites whitelisted for access before the user is authenticated. Prior to enabling the Social Login feature, the walled garden will need to be configured for each of the respective social network.

Facebook and twitter

Add the following entries to the Walled Garden section of the Captive Web Portal profile.

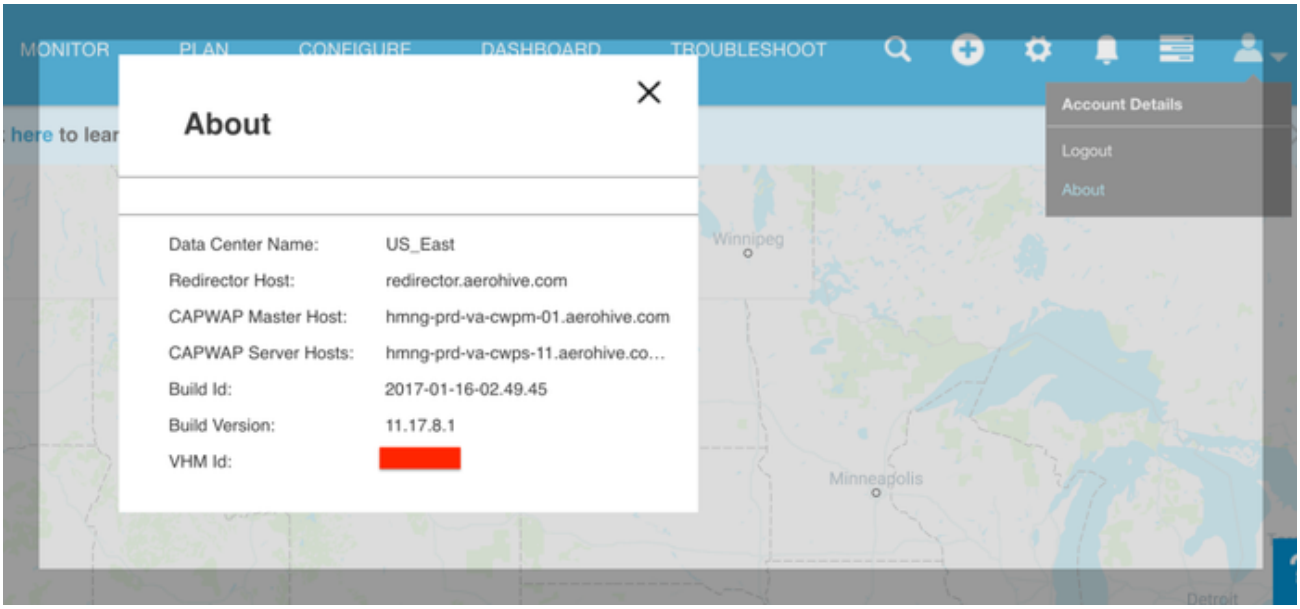
- *.facebook.com
- *.facebook.net
- *.fbcdn.net
- *.akamaihd.net
- www.facebook.com
- *.twitter.com
- *.twimg.com

Presence Data Forwarding

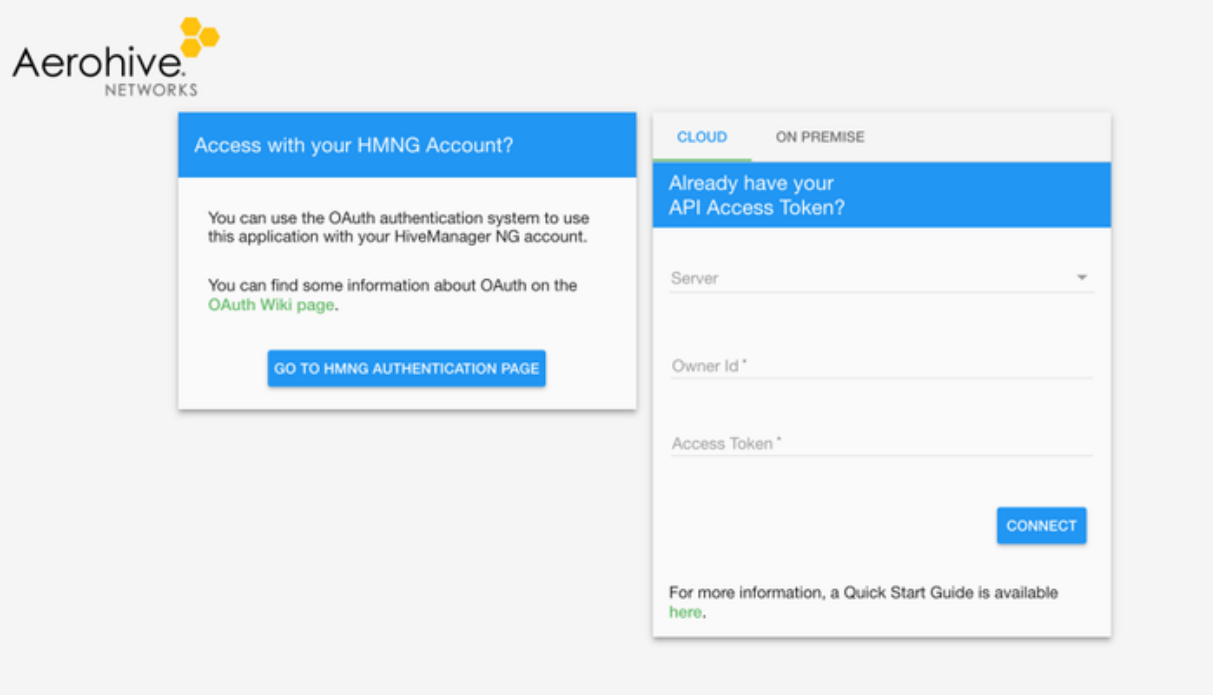
To enable Presence data forwarding on HiveManager NG please complete all steps listed below:

Setting up Presence Webhooks for location data forwarding on HiveManager NG

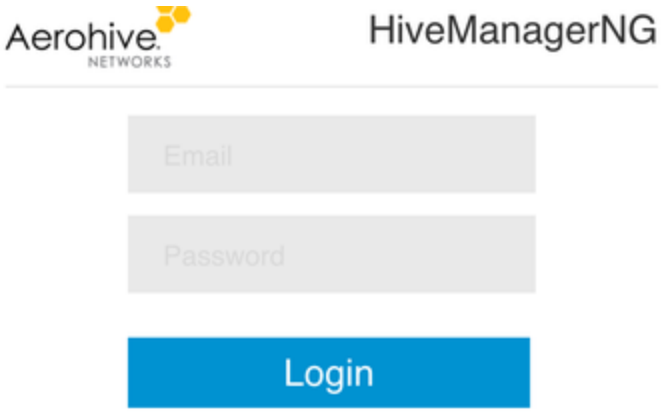
1. Find out your HiveManager's Owner Id and send it to your Zenreach Account Manager. The Owner ID is also called the VHM-Id which can be found on the "About" screen which can be reached by hovering over the icon at the top right. Make a note of this ID and submit it to Zenreach to be forwarded to Aerohive. This ID is used in a currently manual step to enable the presence webhooks on Aerohive's data center by Aerohive's engineering team.



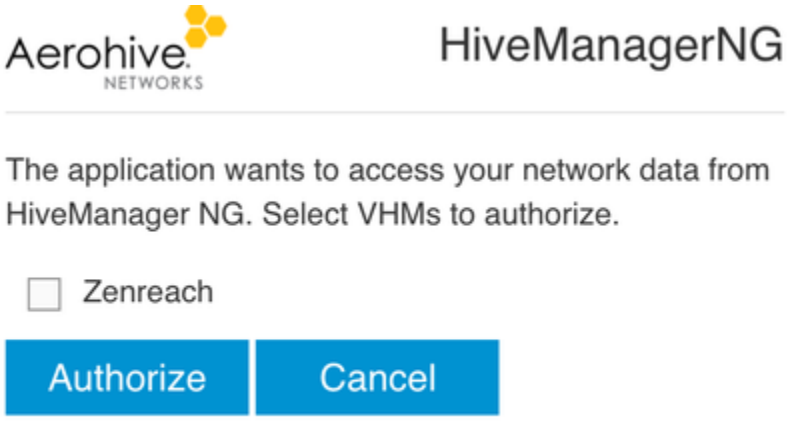
2. Set up the endpoints for the webhooks.
   a. Go to https://check.ah-lab.fr which is a UI web tool created by Aerohive for self subscription to the presence webhooks using API calls with access tokens granted through OAuth. Click **`GO TO HMNG AUTHENTICATION PAGE`**.


Aerohive
NETWORKS
Access with your HMNG Account?
You can use the OAuth authentication system to use this application with your HiveManager NG account.
You can find some information about OAuth on the OAuth Wiki page.
GO TO HMNG AUTHENTICATION PAGE
CLOUD
ON PREMISE
Already have your API Access Token?
Server
Owner Id *
Access Token *
CONNECT
For more information, a Quick Start Guide is available here.

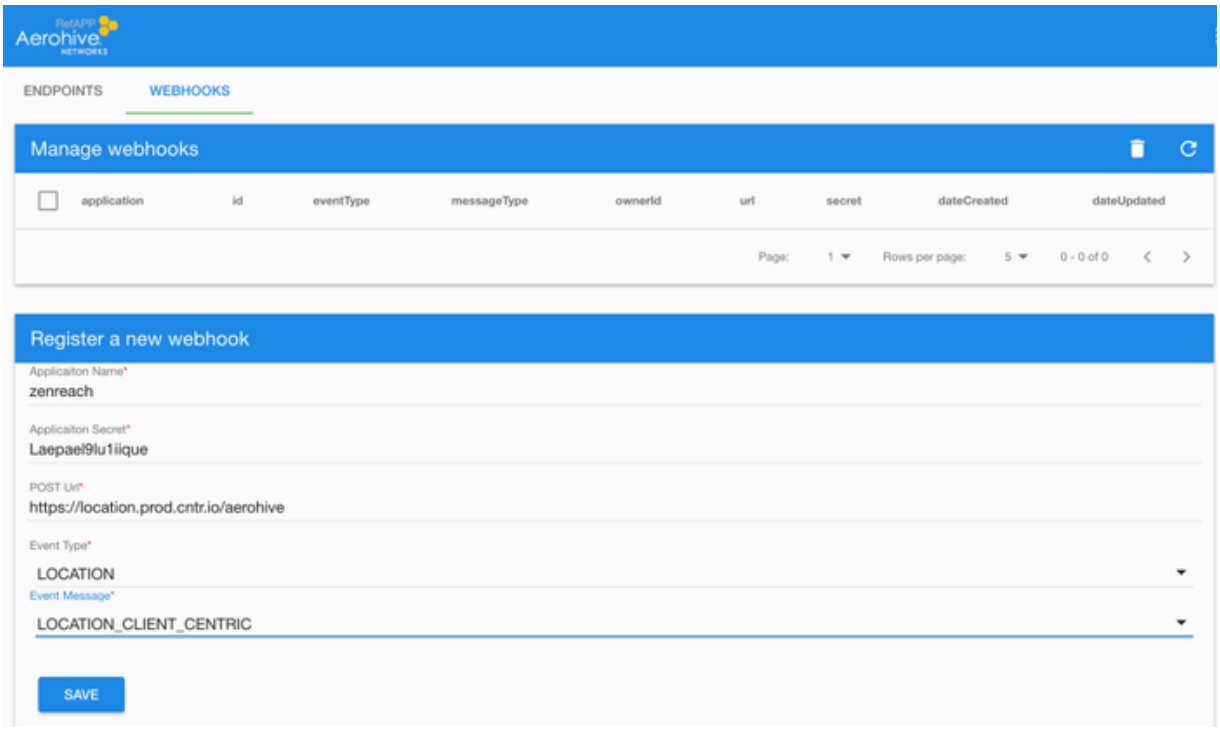
   b. Enter your HiveManager NG credentials for Authentication.



c. Check your organization and click **`Authorize`** to allow the web app to make API calls on behalf of your organization. [In the screenshot below, the org is called "Zenreach" but you should see the name of your own org, *not* "Zenreach".]

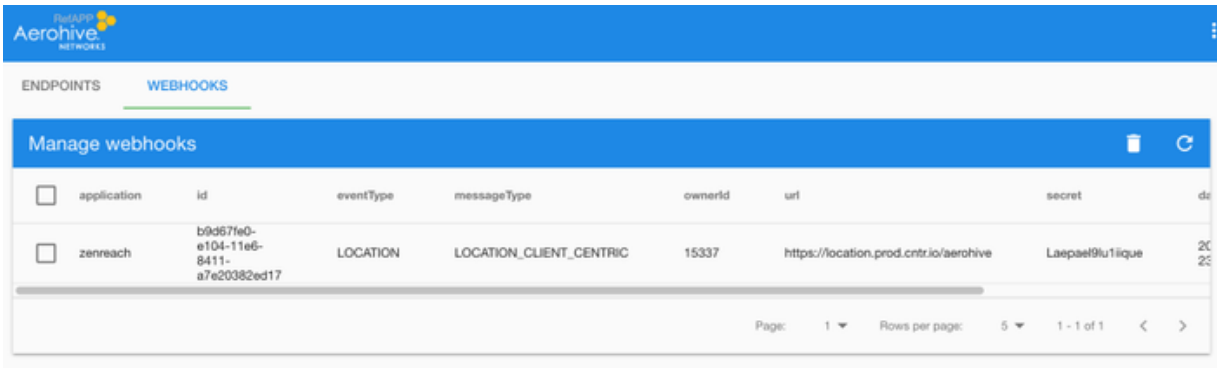


d. Go to the **`WEBHOOKS`** tab at the top left of the screen, scroll down to **`Register a new webhook`** and fill the form with the following information and press save when done.



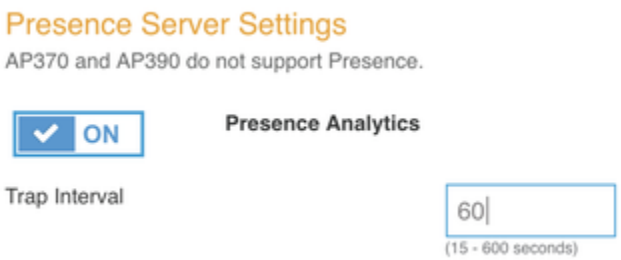
e. **Application Name**: zenreach
Application Secret: Laepael9lu1iique
Post Uri: https://location.prod.cntr.io/aerohive
Event Type: LOCATION
Event Message: LOCATION_CLIENT_CENTRIC

f. Save and you should see an entry appear under **`Managed webhooks`**.



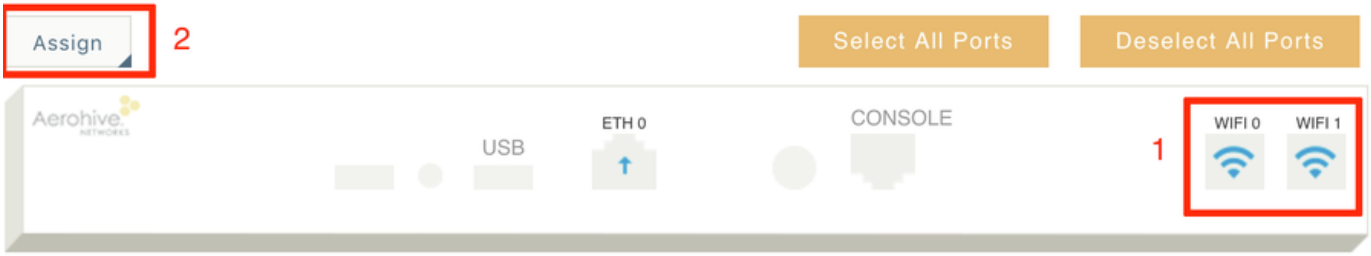
3. Lastly, navigate back into HiveManager and complete the following sequence of steps:

First, create a new radio profile. Navigate to **`Configure`** - **`Common Objects`**, and from the left hand side menu, select the **`Radio Profiles`** menu item under **`POLICY`**. Clone the radio profiles you currently are using. Then, for each of the newly created profiles, edit them and enable the **`Presence Server Settings`** option at the bottom of the page. Set the **`Trap Interval`** to **`60`** (seconds).



Next, assign the new radio profiles to your network policy. Navigate to **`Configure`** - **`Network Policies`**, select your policy, then click **`Wireles`**

s Settings tab at the top. Click **Device Templates**, click your template to edit, then assign the new radio profiles. To assign a radio profile, click one of the wifi icons on the image of the AP (step 1 on image below) and then click **Assign** (step 2 on image below), **Choose Exisiting**, and then choose the radio profile you created.



Make sure you save your configuration and update your devices.